

Review on qudits production and their application to Quantum Communication and Studies on Local Realism

Marco Genovese* and Paolo Traina†

I.N.R.I.M – Istituto Nazionale di Ricerca Metrologica

Strada delle cacce, 91 10135 Turin (Italy)‡

(Dated: February 5, 2008)

The codification in higher dimensional Hilbert Spaces (whose logical basis states are dubbed qudits in analogy with bidimensional qubits) presents various advantages both for Quantum Information applications and for studies on Foundations of Quantum Mechanics.

Purpose of this review is to introduce qudits, to summarize their application to Quantum Communication and researches on Local Realism and, finally, to describe some recent experiment for realizing them.

A Little more in details: after a short introduction, we will consider the advantages of testing local realism with qudits, discussing both the 3-4 dimensional case (both for maximally and non-maximally entanglement) and then the extension to an arbitrary dimension. Afterwards, we will discuss the theoretical results on using qudits for quantum communication, epitomizing the outcomes on a larger security in Quantum Key Distribution protocols (again considering separately qutrits, ququats and generalization to arbitrary dimension). Finally, we will present the experiments performed up to now for producing quantum optical qudits and their applications. In particular, we will mention schemes based on interferometric set-ups, orbital angular momentum entanglement and biphoton polarization. Finally, we will summarize what hyperentanglement is and its applications.

Keywords: quantum communication, Bell inequalities, QKD

*Electronic address: m.genovese@inrim.it

†Electronic address: p.traina@inrim.it

‡URL: <http://www.iem.it/ft/qm/index.shtml>

I. INTRODUCTION

Over the last decade, the possibility of manipulating single quantum states as atoms or photons has largely increased opening, on the one hand, new interesting possibilities in testing the Foundations of Quantum Mechanics and, on the other hand, originating new disciplines as Quantum Information, which studies the encoding, processing (Quantum Computation) and transmission (Quantum Communication) of information using the properties of quantum states, with promising advantages over classical systems.

In particular, Quantum Communication has peculiar characteristics. Purely quantum operations include, for instance, Quantum Key Distribution (QKD), quantum teleportation, quantum dense coding and entanglement swapping. These protocols stem from purely quantum properties characteristics of Quantum Mechanics (QM), as the uncertainty principle, the superposition principle, entanglement (i.e., the existence of states whose wave function cannot be factored in single particle wave functions) and the no-cloning theorem. The possibility of the totally secure communication of a cryptographic key (QKD) is of the utmost interest in the present society, based on a widespread communications network. In fact, the specific characteristics of QM allow a demonstration of absolute security in communication based on quantum states. The basic principle of QKD is sharing, by transmitting quantum states, a random secret key between two distant parties. Various QKD protocols have been proposed, each with its own advantages and disadvantages. Most of them encode the information in a state which is defined in a two dimensions Hilbert space (i.e., in a quantum bit, called qubit). However, security can be increased by codifying in higher dimensional Hilbert spaces (qudits).

Also in the researches on Foundations of Quantum Mechanics the use of qudits presents advantages, in particular in relation to the studies on local realism.

Incidentally, as we will discuss later, these two seemingly rather distant fields of research are tightly related to each other.

Purpose of this review is to introduce qudits (giving a wide bibliography on them), to summarize their application to Quantum Communication and Studies on Local Realism and, finally, to describe some recent experiment for realizing them. A Little more in details: In section II, we will consider the advantages of testing local realism with qudits, discussing both the 3-4 dimensional case (both for maximally and non-maximally entanglement) and then the extension to an arbitrary dimension. In section III we will present the theoretical results on using qudits for quantum communication, epitomizing the outcomes on a larger security in Quantum Key Distribution protocols (again considering separately qutrits, ququats and generalization to arbitrary dimension). Finally, in section IV we

will introduce the experiments performed up to now for producing quantum optical qudits and their applications. In particular, we will mention schemes based on interferometric set-ups, orbital angular momentum entanglement and biphoton polarization; then, finally, we will summarize what hyperentanglement is and its applications.

II. VIOLATIONS OF LOCAL REALISM FOR QUDITS

The quest for local realistic alternatives to QM has a pluridecennial history, stemming from the 1935 Einstein-Podolsky-Rosen paper¹, where completeness of QM was questioned. Bell Inequalities (BI's)^{2,3,4} set a limit on the ability for any theory based on local realistic (LR) assumptions to reproduce all the statistical results predicted by QM. Even if many experiments show violation of BI's, no conclusive experimental test on local realism has been performed yet, because those results rely on the accessory assumption that the very few events observed, due to the finite (and often low) efficiency of real detection apparatuses, are a faithful statistical sample (this issue is often called *detection loophole*)^{5,6,7,8}. This means that the possibility to find a Local Hidden Variable Theory (LHVT) describing the quantum world (to which standard Quantum Mechanics could be just an approximation) is not definitely discarded. At the moment, only a detection loophole free experiment has been performed with Be ions⁹, but without fulfilling the space separation requirement imposed in the original EPR argument¹. In order to close the detection loophole one should have a detecting apparatus characterized by a minimum detection efficiency η^* whose value depends on the specific measurement procedure and on the amount of local realism violation predicted by Quantum Mechanics. As far as two-level quantum objects are concerned, it has been estimated that a minimum quantum efficiency $\eta^* = 82.84\%$ is needed for a detection loophole free test for maximally entangled qubits and that this value can be lowered to $\eta^* = 66.7\%$ for non-maximally entangled qubits (see^{10,11} and references therein).

In recent works it has been suggested^{12,13,14} that violation of local realism for *qudits* is expected to grow with d and this leads to a smaller required η^* . In this sense it is interesting to explore Hilbert spaces with dimension $d \geq 2$. Incidentally, it is also worth to mention that the quantification of violation of local realism is also related to the quantification of entanglement as a resource for quantum information^{5,15}.

A. Violation of Local realism for $d = 3, 4$

The first papers exploring the possible violations of local realism by qutrits (due to Kaszlikowski *et al.*)^{16,17} were centered on the following scenario. Let us assume that the global state shared by two parties A and B is a three-

dimensional maximally entangled state as:

$$|\psi_{in}\rangle = \frac{1}{\sqrt{3}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B + |2\rangle_A|2\rangle_B). \quad (1)$$

Now let both the parties send their particles through two similar devices called *unbiased 6-ports BeamSplitters* (aka tritters)¹⁸. These are a three-dimensional generalization of a 50%/50% Beam Splitter, whose output state in response to one of the three inputs is a weighted superposition of its three eigenstates, so that the global effect, for instance, on particle A (B) defines a unitary transformation with the followings entries:

$$U_{kl}^A(\vec{\phi}^a) = \frac{1}{\sqrt{3}}e^{i(\frac{2\pi}{3}kl+\phi_l^a)} \quad (U_{kl}^B(\vec{\theta}^b) = \frac{1}{\sqrt{3}}e^{i(\frac{2\pi}{3}kl+\theta_l^b)}) \quad k, l = 0, 1, 2. \quad (2)$$

In the last equation, the formal vector $\vec{\phi}^a$ ($\vec{\theta}^b$) refers to one of two possible (identified by the value a (b) of the upper index) settings of three phase shifts used by A (B). For instance, $\vec{\phi}^1 = (\phi_0^1, \phi_1^1, \phi_2^1)$ ($\vec{\theta}^1 = (\theta_0^1, \theta_1^1, \theta_2^1)$). The probability $P(A_a = k, B_b = l)$ of a given outcome for the two quantities observed by A and B is calculated by projecting the global output state on $|k\rangle_A|l\rangle_B$.

A measure of the strength of the violation of local realism was defined as the minimal noise admixture F_{max} ¹⁹ to the state below which no LHV can reproduce the correlation results. The general model of the mixed qutrit state is

$$\rho_{noise} = (1 - F)|\psi\rangle\langle\psi| + \frac{F}{9}\mathbf{1} \quad (3)$$

where $0 \leq F \leq 1$ and $\mathbf{1}$ is the three-dimensional identity matrix.

In a first paper¹⁶, it is proven analitically that, for the described set of trichotomic observables with a specific choice of the phase shifts $(\vec{\phi}^a, \vec{\theta}^b)$, one has

$$F_{max} = \frac{11 - 6\sqrt{3}}{2}, \quad (4)$$

while for maximally entangled qubits this value is smaller ($\frac{2-\sqrt{2}}{2}$). Thus, entangled qutrits are more robust against LR description than entangled qubits.

It must be pointed out that those results concern the computation of correlation functions. In order to have a necessary and sufficient condition for the existence of local hidden variables, more strong constraints on outcome probabilities are needed, such as in CH inequality³. A general CH inequality¹⁷ for qutrits has been proposed as

$$\begin{aligned}
& P(A_1 = 2; B_1 = 1) + P(A_1 = 2; B_2 = 1) - P(A_2 = 2; B_1 = 1) + P(A_2 = 2; B_2 = 1) + \\
& P(A_1 = 1; B_1 = 2) + P(A_1 = 1; B_2 = 2) - P(A_2 = 1; B_1 = 2) + P(A_2 = 1; B_2 = 2) + \\
& P(A_1 = 2; B_1 = 2) + P(A_1 = 1; B_2 = 1) - P(A_2 = 2; B_1 = 2) + P(A_2 = 2; B_2 = 2) - \\
& P(A_1 = 1) - P(A_2 = 2) - P(B_2 = 1) - P(B_2 = 2) \leq 0.
\end{aligned} \tag{5}$$

Numerical calculations on the outcome probabilities yield results that are equivalent to the previous ones for what concerns maximal noise admixture and consequently robustness against LR description.

Prompted by the results in qubits case¹⁰, computations about the behaviour of more general non-maximally entangled qutrits^{20,21} have been successively performed. It has been shown that non-maximal entangled qutrits exist which violate local realism more strongly than maximal entangled ones (see **Fig. 1**). It can also be shown that differences between the violations of LR in the two cases increase with the dimension of the system. It is also worth mentioning that it is always possible to obtain any of these maximally “non-LR” states from the maximally entangled one via *local operations* and *classical communication* (LOCC).

Fig. 1

Similar considerations can be extended to the 4-dimensional Hilbert Space²² (several experiments related to the measure of Bell Inequalities in three and four dimensions have been recently performed^{23,24,25,26} and will be discussed later). The calculated values of η^* and F for $d = 2, 3, 4$ are reported on table 1 and table 2, respectively.

Table 1

Table 2

B. Violation of local realism for arbitrary dimension

In one of the previously cited works²⁰ it was inferred that the violation of local realism increases with the dimension of the system. In order to investigate this tendency of entangled qudit systems, a general class of Bell Inequalities for arbitrary dimension states have been proposed by Collins *et al.* in 2002²⁷. This $CGLMPI_d$ inequalities (whose maximal values are limited by 2 for any LHV models) are obtained starting from some logical constraints that the correlation function must satisfy for any local variable theory, following an approach similar to the one leading to standard CHSH inequality⁴, to which, by the way, $CGLMPI_2$ is equivalent. Also the values of the violations of such inequalities by maximally entangled qudits are calculated for $d \geq 2$

$$CGLMPI_d(|\psi_{m.e.}\rangle) = 4d \sum_{k=0}^{\frac{d}{2}-1} \left(1 - \frac{2k}{d-1}\right) \left(\frac{1}{2d^3 \sin^2[\frac{\pi}{d}(k + \frac{1}{4})]} - \frac{1}{2d^3 \sin^2[\frac{\pi}{d}(\frac{1}{4} - k - 1)]} \right) \quad (6)$$

showing that the robustness of these states against LR description increases with d .

An asymptotic limit for $d \rightarrow \infty$ is also extrapolated ($CGLMPI_\infty=2.296981$).

A more detailed investigation on the structure of such inequalities is due to Chen *et al.*²⁸ who, in their 2005 – 2006 works, calculated maximal violations and the corresponding eigenstates for d up to 8000. The sets of observables considered there are the extensions to any dimension d of the unitary transformations proposed by Kaszlikowski *et al.*^{16,17} and the results are obtained by maximizing the eigenvalues of the Bell operator. All the results are in agreement with the previously cited papers and also, since it is clearly evident that LR violations grow with d , it is calculated that maximal violations are obtained once again for non-maximally entangled qudits. Furthermore, an empirical formula linking maximal violation value to d and a family of convenient approximate states are introduced.

III. QUDITS & QUANTUM COMMUNICATION

Quantum Communication is the branch of Quantum Information Theory dealing with the exchange of information among remote parties when this information is encoded by means of some physical properties of a quantum object (*e.g.*, single photon's polarization)²⁹. The most straightforward applications in this field concern Quantum Cryptography³⁰.

In the most common scenario, a party, traditionally dubbed Alice (A), wants to share some reserved information with a trusted receiver, called Bob (B) and, in order to protect the security of the communication against some malicious eavesdropper's (E) attacks, they apply a *one-time pad* protocol (aka *Vernam Cypher*). For this task they need, for each message, a system to share a totally random key string (in principle of the same length of the message). This is possible by means of Quantum Key Distribution protocols, with which A and B, only by virtue of the laws of Quantum Mechanics, are able to produce perfectly correlated (and unique) random strings to be used as encryption (or decryption) key over messages exchanged in a public channel. Two main QKD classes are known.

The first class stems from a protocol proposed by Bennet and Brassard in 1984³¹ (BB84). In the original proposal, A encodes her key bits by means of the polarization states of single photons (for instance, vertical polarization corresponding to 0 and horizontal one corresponding to 1), randomly switching between two *mutually unbiased* bases, such as $\{|H\rangle, |V\rangle\}$ and $\{|\frac{\pi}{4}\rangle, |-\frac{\pi}{4}\rangle\}$. B receives via a Quantum Channel the qubits and he projects their polarization states on either of the two bases, randomly as well. As a result, when A and B use the same basis they get perfectly

correlated bits, while they get stochastic outcomes in the other cases. If E is present, She can try to intercept A's photons, measure them and send to B the eigenvector corresponding to the measured value. When this strategy (*intecpt-resend*) is used, it can be shown that E's intervention modifies the probabilistic properties of B's string, resulting in a increased Quantum Bit Error Rate (QBER) and a reduced average mutual information shared by A and B (I_{AB}). More sophisticated attacks can also be envisaged, for example E could entangle some probes to the transmitted qubits and perform a measurement on them in a second time (coherent attack). In general it can be proved that A and B can extract a secret key from a corrupted one simply by classical algorithms (such as *error correction* and *privacy amplification*) if the amount of their mutual information I_{AB} is bigger than E's one (I_{EA} , I_{EB}).

The second class, related to a protocol first proposed by Ekert³² (Ekert91), uses the correlations shown by entangled qubits as a guarantee of the confidentiality of the communication. In this case, A and B are separately given one of the two parties of a entangled bipartite system, and they randomly (and independently) project their qubits like in BB84. Since E's presence spoils entanglement between A's and B's photons, whenever certain BI is not violated by randomly chosen subsets of their strings, communication is rejected, since it can be proven that the communication becomes unsecure in this condition.

Many experimental implementations of QKD protocols with qubits have been performed. In this section we will briefly review the major advantages stemming from the extension to arbitrary dimension Hilbert spaces^{33,34}.

A. QKD with qutrits

The immediate extension of BB84 protocols for qutrits has been proposed by Bechmann-Pasquinucci and Peres in 2000³³. In a 3-dimensional Hilbert Space there are four possible *mutually unbiased bases* (MUOB's), corresponding to 12 vectors. Assuming the first base is

$$\{|\alpha\rangle, |\beta\rangle, |\gamma\rangle\}, \quad (7)$$

the second is given by its discrete fourier transform

$$\left\{ \frac{1}{\sqrt{3}} (|\alpha\rangle + |\beta\rangle + |\gamma\rangle), \frac{1}{\sqrt{3}} (|\alpha\rangle + e^{2\frac{\pi}{3}i}|\beta\rangle + e^{-2\frac{\pi}{3}i}|\gamma\rangle), \frac{1}{\sqrt{3}} (|\alpha\rangle + e^{-2\frac{\pi}{3}i}|\beta\rangle + e^{2\frac{\pi}{3}i}|\gamma\rangle) \right\} \quad (8)$$

and the other two bases can be written as

$$\frac{1}{\sqrt{3}} (e^{\pm 2\frac{\pi}{3}i}|\alpha\rangle + |\beta\rangle + |\gamma\rangle), \quad (9)$$

and cyclic permutations. A chooses randomly one of those vectors and sends it to B, who measures the state projecting on one of the four possible bases randomly as well. After that, B publicly reveals the basis used but not the outcome. If the bases are equal, A and B share a trit of information, otherwise they get fully uncorrelated results which are immediately discarded. A and B perform as many iterations as they can in order to get a key of satisfactory length before proceeding with error correction and privacy amplification schemes (with sums *modulo* 3 instead of parity checks). In this case, considering a simple *intercept-resend* attack, E gets on the average $1/4$ of a trit of information for every transmission, while B error rate grows to $1/2$ (compared, respectively, to $1/2$ bit and to $1/4$ in the qubit case). This protocol, compared with more complex ones, appears to be optimal for this kind of attack in the case of “one way” communications, since it gives the the lowest value of mutual information gained by E for a given quantity of information shared between A and B and the authors infer it to be optimal also for more sophisticated eavesdropping strategies.

Another possibility is to exploit 3-dimensional BIs to perform Ekert91-like protocols as proposed in³⁵. The proposed setup is the same as the one previously introduced to describe Kaszlikowski’s CH inequality for qutrits and A and B, after the transmission and the public declaration of the sets of phase shift used, perform the calculation of the quantity on left side of eq. (5) on a subset of their results. If maximal violation of local realism is not reached they assume that something (E or noise) had disturbed the transmission, otherwise they extract the key from the remaining data. The authors show that, for a symmetric incoherent attack in which E controls the source of entangled qutrits, the correlation in the results between A and B is reduced of a factor depending on the initial state prepared by E and on the ancilla state used. E must keep this factor under a certain threshold value $((6\sqrt{3} - 9)/2)$ in order to be unnoticed, otherwise her presence will spoil the BI violation. But computations yield that, in the region in which local realism is violated, E’s average error rate is always bigger than B’s one and the mutual information I_{AB} shared by A and B is always greater than information leaked to E (which is a condition for secret key extraction). As a closing remark it is pointed out that this kind of protocol is also more robust to noise than standard ones (Ekert91 and BB84) tolerating a noise admixture of 33.7% (against 29.2%).

B. QKD with ququats

A BB84-like protocol with ququats can be performed³⁶ with A choosing randomly among eight states belonging to two mutually unbiased orthogonal bases of H_4 . Also in this case, given the first basis $\{|\alpha_i\rangle\}$, the second one $(\{|\beta_j\rangle\})$ can be obtained as discrete fourier transform of the latter. Without E, if n ququats are sent, on the average B guesses

the right base in one half of the cases, so that $n/2$ shared “quats” (n bits) are perfectly correlated. If E adopts a standard *intercept-resend* strategy, it is easy to show that on the average she gets half of the transmitted bits, just like in the analogous protocol in 2 dimensions, but indeed E’s presence induce a greater disturbance in the communication leading to an error rate in B’s results larger than in the qubit case ($3/8$ against $1/4$). Even if E uses an intermediate basis $\{|\gamma_i\rangle\}$ such that

$$|\langle\gamma_i|\alpha_i\rangle| = |\langle\gamma_i|\beta_i\rangle| = MAX \quad , \quad |\langle\gamma_i|\alpha_j\rangle| = |\langle\gamma_i|\beta_j\rangle| = MIN, \quad (10)$$

it can be shown that the average information leaked is less than a bit (0.792) for each ququat transmitted and that the error rate introduced is even larger than in the previous case ($5/12$).

C. Generalization to arbitrary dimension

A suitable generalization³⁷ of the BB84 protocol using quantum d -level states, with d an arbitrary integer, can be realized following two ways. The first is to use only two mutually unbiased orthogonal bases of H_d (as in standard BB84), while the second exploits all $d + 1$ possible such bases (as in six-states protocol). In both cases we suppose E owns some sort of cloning machine (which must be considered imperfect due to no-cloning theorem), used to copy the intercepted qudits before sending them to B. Obviously this procedure adds a degree of mixedness to A and B bipartite state. Let’s firstly assume a protocol with only 2 complementary bases. If E strategy is based on individual attacks, the best she can do (as in the qubit case) is to use a cloner that copies equally (with equal fidelity F_E) both bases. Applying this constraint to a general class of cloning transformations³⁸ and maximizing E’s fidelity, it can be shown that the information stolen by E equals the one shared by the authorized parties when

$$F_E = F_B = \frac{1}{2} \left(1 + \frac{1}{\sqrt{d}} \right) \quad (11)$$

According to the known criterion this also gives the maximum noise admixture $D = 1 - F$ below which the extraction of secret key via privacy amplification is possible. This result suggests that communication security grows with the dimension of the carrier quantum state.

Following an analogous approach, it can be shown that in the case in which all $d + 1$ MUOB’s are used (which are known only when d is some power of a prime number) there is a slight improvement in the sense that for a given fidelity F , I_{AB} is somewhat bigger and so is the maximum noise treshold D , thus the protocol is more robust than the previous one.

Also the case of coherent attack in which E performs a collective measurement on arbitrary long qudit strings is considered and it is found that the upper bound to disturbance D in this case equals the value which is known for coherent attacks on strings of qubits³⁹.

Similar studies has been devoted to the investigation of possible extension of Ekert91 protocol to arbitrary dimension and its security against a wide class of attacks⁴⁰. Also in this case an increased robustness against noise is found with respect to the standard qubit protocol.

IV. IMPLEMENTATIONS

In this section we briefly review some major recent works on the generation and exploitation of experimental entangled qutrits and ququats for Quantum Communication purposes and LR tests. Although the most of the reported schemes use single photons as carriers, these applications rely on different physical implementations corresponding to the different possible degrees of freedom to be used in encoding the information.

A. Postselected four-photon states

In 2002, in order to give an experimental demonstration of the violation of CHSH inequality for spin-1 objects, polarization-entangled four-photon states produced by Type-II PDC⁴¹ were studied²⁵. These states, which are present in the second order component of the downconverted field

$$\frac{1}{\sqrt{3}}(|HH, VV\rangle + |HV, VH\rangle + |VV, HH\rangle), \quad (12)$$

are by all means four-photon qutrits and they can be observed by postselection techniques.

The polarization state was analysed with a setup similar to traditional Stern-Gerlach apparatus for spin-1 particles measurement and violation of CHSH inequality by more than 13 standard deviation was observed.

B. Interferometric schemes

A first possible implementation of energy-time entangled qutrits for QKD is reported by Thew *et al.*²⁴. In their scheme (an extension of Franson one⁴² for qubits), they use the superposition state of the three possible paths of a single photon in a 3-arm interferometer as qutrit source.

Photons, obtained via Parametric Down-Conversion⁴¹ produced by a Periodically Poled Lithium Niobate waveguide,

are coupled to monomode optical fiber and then sent to an all-fiber system which separates the photon pairs (by a beam splitter) and addresses each of them to a different 6 – *port* Michelson interferometer, working as a tritter. The phase on each arm of those tritters can be controlled via temperature. The path length differences between the two interferometers are taken to be equal and care is also taken to avoid polarization drift of photons inside them. By six detectors (three for each interferometer) can be observed nine possible combination of detection times distributions corresponding to the possible stories of the produced photon pair. These are reproduced in a histogram whose central peak represents the case in which both take the same path in each tritter (the detection times coincide). Because the path length differences in the interferometers are much smaller than coherence length of the pump beam, no information is available on creation times of photons or on the path taken, so interference effects are detected (with visibility $V = 0.919 \pm 0.026$).

The authors claim to be able to produce high symmetry, maximally entangled qutrits. Full characterization of the generated states is performed and the declared fidelity is $F = 0.985 \pm 0.018$.

A similar scheme can be used to produce generalized GHZ states in three or four dimensions⁴³.

Raising the dimension of this kind of scheme could be unpractical because it would require more than three armed interferometers (anyway hyperentanglement could help).

An interesting scheme to produce high dimensional time-bin entangled biphoton states has been proposed in 2005⁴⁴. Here a train of pulses generated by a mode-locked laser pumps a nonlinear crystal. Since no information is available on the creation time of photon pairs, the state created is of the form

$$|\psi\rangle = \sum_{j=1}^N c_j e^{i\phi_j} |j, j\rangle \quad (13)$$

where j labels the time-bin, c_j are constant probability amplitudes, ϕ_j are the constant phase shifts between successive pulses and N is the number of pulses. The state is then analyzed by a 2-photon Fabri-Perot interferometer to demonstrate high order entanglement. In this experiment the dimension is limited only by the phase coherence between subsequent pulses and could, in principle, be very large, even if it must be remarked that experimental difficulties increase significantly as the dimensionality grows.

C. Orbital angular momentum entanglement

In 2002²³ Vaziri *et al.* have demonstrated for the first time entanglement between qutrits using the Orbital Angular Momentum of photons (which is conserved during PDC process⁴⁵). In this case the three possible eigenstates of OAM

$(0, \hbar, -\hbar)$ span the qutrit space. After that a PDC pair is created, each of the photons is addressed to an holographic module (consisting of two displaced holograms) which can transfer the incoming mode into a desired superposition LG_{0l} LaGuerre-Gaussian Modes (each carrying $l\hbar$ per photon). After the state is generated, each mode is sent to a device which can discriminate among LG_{0l} modes.

Using this scheme, a violation of more than 18 standard deviations of CGLMP inequality for three dimensions has been measured, corresponding to non-maximally OAM entangled state.

Two years later⁴⁶ complete characterization of OAM entangled qutrits has been provided by Quantum Tomography measuring the amount of entanglement and the degree of mixture and it has been shown how to exploit such states for Quantum Communication (Quantum bit commitment) with high security.

Finally, Ren *et al.* experimentally showed that high-dimensional OAM entanglement of a pair of photons can be survived after a photon-plasmon-photon conversion, the information of the spatial mode being thus coherently transmitted by surface plasmons⁴⁷.

D. Biphoton qudits

Since the experimental Quantum Information scene is dominated by the generation, control and detection of polarization entangled biphoton states, the most natural experimental ground to reliably expand this discipline in more than two dimensions could be the generation of polarization entangled qutrits and ququats. It should also be underlined that this kind of states are definitely easier to control than the previously described ones because only linear optical elements are needed. On the other hand, to experimentally tune all the superposition amplitudes in order to generate any arbitrary qutrit could be a very complex task if it is to be done by modifying a tritter phase shifts set or producing custom made holograms.

A first scheme addressed to the production of arbitrary polarization qutrit states has been implemented in 2004⁴⁸(see **Fig. 2**) by pumping with a single coherent source three non-linear crystals, essentially overlapping Type-I and Type-II PDC emissions. The system allowed the generation of arbitrary qutrits and 12 states belonging to three mutually unbiased orthogonal bases of H_3 were produced and measured with high fidelity (between 0.9842 and 0.9991). Anyway, this method does not allow to have entangled qutrits.

Fig. 2

A method⁴⁹ to engineer arbitrary pure and mixed states of polarization qutrits and ququats exists for which only a single nonlinear crystal and linear optical elements are needed. In fact it is proven by means of *Singular*

value decomposition theorem that any arbitrary qutrit or ququat can be obtained performing only unitary local transformations on a qubit bipartite *seed* state (in this case a non-maximally entangled polarization biphoton state). Following this line it has been possible to produce and measure with high average fidelity (0.93) four MUOB's in H_3 and, in principle, five MUOB's in H_4 (20 states) can be observed as well.

Furthermore, an experimental way to produce and measure polarization ququarts based on non-degenerate biphoton field for QKD purposes has been lately suggested⁵⁰.

In 2005 Neves *et. al.* showed to be able to achieve entangled biphoton qudits ($d = 4,8$) also by means of the transverse spatial correlation between SPDC photons⁵¹. According to their scheme, Down-Converted photons are sent to two identical apertures with d slits and the d possible paths (one for every slit) taken by each of the photons define the qudit space. For a proper adjustment of the pump beam, it is possible to have the two photons passing only by symmetrically opposite slits so that entanglement between the transverse spatial modes is obtained. The state has been generated and measured with high fidelity and it is proven to be a pure entangled state.

Finally, Ren *et. al* showed that the Hermite-Gaussian (HG) modes of SPDC downconverted beams are quasi-conserved and that the generated multidimensional biphoton states are HG modes entangled for some special cases⁵².

E. Hyperentanglement

A Hyperentangled state is a quantum system which is entangled simultaneously in more than one of its degrees of freedom. Experimental generation of such states is interesting not only because they can be seen as qudits to be used for tests on violations of local realism⁶³ or QKD purposes, but also since Hyperentanglement, as it has been suggested⁵⁴ and successively experimentally proven⁵⁵, can provide a control qubit for complete Bell state discrimination with linear optical elements.

As an extension to a simple yet elegant scheme proposed by Brendel *et al.* in 1999⁵⁷ for producing energy-time entanglement, a source of energy-time and polarization Hyperentangled biphoton states is proposed by Genovese and Novero⁵⁸ (see **Fig. 3**).

A single photon pulse feeds a Mach-Zender interferometer in order to generate, if the pulse duration is much smaller than the path length difference between the *short* and the *long* arm, a superposition state which reads:

$$\alpha|short\rangle + \beta|long\rangle, \tag{14}$$

where the complex amplitudes of the superposition α and β are determined respectively by the coupling ratios at the beam splitters and the phase difference introduced between the two arms. If the previous photon pumps a non-linear crystal, polarization entanglement can also be generated via PDC, resulting in a global output biphoton state which can be written (for instance in the type-II case) as

$$(\alpha|short\rangle + \beta|long\rangle) \otimes \frac{1}{\sqrt{2}}(\gamma|HV\rangle + \delta|VH\rangle), \quad (15)$$

where V and H label respectively vertical and horizontal polarization.

In order to observe interference in the time domain, one should compensate for timing information introduced by the pulsed regime. This is achieved by using other two identical interferometers as detection apparatus, one for each PDC arm. Temporal indistinguishability in this case is recovered by postselecting the central detection peak out of the three possible, corresponding to those events in which both downconverted photons of a pair travel along the alternative arm with respect to the one taken by the corresponding pump photon.

The proposed scheme can be used for implementations of QKD protocols, entanglement swapping, teleportation and generation of 3-photon GHZ states.

Fig. 3

Other ways⁴³ to combine known and efficient entanglement sources to generate hyperentangled systems can be thought: for instance, one can in principle exploit simultaneously energy-time (via interferometers) and OAM entanglement.

Also the previously discussed scheme by Mataloni *et al.* can be extended by means of hyperentanglement⁵⁵. This is done by a four-holes screen which allows to select two complementary pairs of momentum modes from the incoming polarization entangled biphoton field.

Finally, recently polarization-momentum hyperentanglement has been used to perform experimental *all versus nothing* non-locality tests for bipartite four-dimensional entangled states^{26,56,59}, *i.e.* a demonstration of non statistical predictions by quantum mechanics on the properties of GHZ states.

V. CONCLUDING REMARKS

We have presented an introductory review on the codification of quantum information in higher dimensional Hilbert spaces ($d > 2$, qudits) and application to quantum communication and studies of local realism, both from a theoretical

and experimental point of view.

The results achieved up to now, and presented here, show that this field of research is very promising for both these applications.

All the qudits realizations produced up to now are based on photonic states. This is rather obvious when one is thinking to applications to quantum communication and studies on local realism, where in general quantum optical states play the game. Next steps will be on the one side the development of efficient sources of photonic qudits and on the other side the implementation of long distance quantum communication channels where advantages of qudit respect to qubit codification are exploited. Also an attempt to finally reach a loophole free test of local realism could take advantage by the reduced limit quantum efficiency required by using qudits.

In conclusion it must also be mentioned that recently new applications of qudits, e.g. to quantum computation⁶⁰ or quantum communication protocols beyond QKD⁶¹, have been proposed⁶⁴. These results could prompt the implementation of qudits on further physical systems as ions, atoms, etc. opening new and unexplored sectors of research in this field.

Acknowledgements: This work was supported in part by the by italian minister of research (PRIN 2005023443-002) and by Regione Piemonte (E14).

Limit efficiency η^* for $d = 2, 3, 4$

η^* (%)	qubits	qutrits	ququats
CH	82.84 (66.7)	82.09 (81.39)	undefined
CGLMP	84.0896	83.4357 (82.8330)	83.0993 (82.0237)

TABLE 1: *Various expected limit quantum efficiencies in order to close detection loophole depending on qudits dimension (the bracketed values concern non-maximal entanglement).*

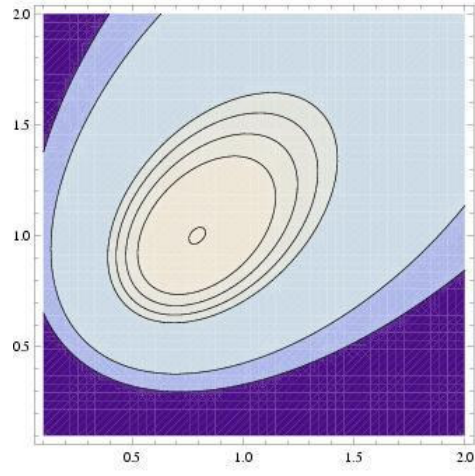


FIG. 1: Contour plot of the left hand side of Eq. 5 calculated with the non-maximally entangled qutrit state

$\Psi = \frac{1}{\sqrt{1+a^2+b^2}} (|0\rangle_A|0\rangle_B + a|1\rangle_A|1\rangle_B + b|2\rangle_A|2\rangle_B)$ in the plane a (abscissa) - b (ordinate). Contour lines are at $-0.15, -0.1, 0, 0.01, 0.02, 0.03, 0.05$.

Resistance to noise F for $d = 2, 3, 4$

	qubits	qutrits	ququats
F_{me}	0.293	0.304	0.309
F_{mv}	0.293	0.314	0.327

TABLE 2: *Resistance to noise for maximal (F_{me}) and non-maximal (F_{mv}) entangled qudits depending on dimension d .*

-
1. A. Einstein, B. Podolsky and N. Rosen, Phys. Rev. 47, 777 **(1935)**.
 2. J. S. Bell, Physics 1, 195 **(1964)**.
 3. J. F. Clauser and M. A. Horne, Phys. Rev. D 10, 526–535 **(1974)**.
 4. J. F. Clauser, M. A. Horne, A. Shimony and R. A. Holt, Phys. Rev. Lett. 23, 880–884 **(1969)**.
 5. M. Genovese, Phys. Rep. 413, 319–397 **(2005)**.
 6. E. Santos, Phys. Lett. A 212, 10 **(1996)**.
 7. L. De Caro, A. Garuccio, Phys. Rev. A 54, 174 **(1996)**.
 8. P. M. Pearle, Phys. Rev. D 2, 1418 **(1970)**.
 9. M. A. Rowe, D. Kielpinski, V. Meyer, C. A. Sackett, W. M. Itano, C. Monroe and D. J. Wineland, Nature 409, 791–794 **(2001)**.
 10. P. H. Eberhard, Phys. Rev. A 47, R747 **(1993)**.
 11. G. Brida et al., Phys. Lett. A 268, 12 **(2000)**; A 299, 121 **(2002)**; M. Genovese et al., Opt. & Spec. 99, 185 **(2005)** and refs therein.
 12. S. Massar, S. Pironio, J. Roland and B. Gisin, Phys. Rev. A 66, 052112 **(2002)**.
 13. S. Massar and S. Pironio, Phys. Rev. A 68, 062109 **(2003)**.
 14. S. Massar, Phys. Rev. A 65, 032121 **(2002)**.
 15. C. Lupo et al., Journ. Phys. A. 40, 13091 **(2007)** and references therein.
 16. J. L. Chen, D. Kaszlikowski, L. C. Kwek, Żukowski and C. H. Oh, Phys. Rev. A 64, 052109 **(2001)**.
 17. D. Kaszlikowski, L. C. Kwek, J. L. Chen, M. Żukowski and C. H. Oh, Phys. Rev. A 65, 032118 **(2002)**.
 18. M. Żukowski, A. Zeilinger and M. A. Horne, Phys. Rev. A 55, 2564 **(1997)**.
 19. D. Kaszlikowski, P. Gnaniński, M. Żukowski, W. Miklaszewski and A. Zeilinger, Phys. Rev. Lett. 85, 4418 **(2000)**.
 20. A. Acin, T. Durt, N. Gisin and J. I. Latorre, Phys. Rev. A 65, 052325 **(2002)**.
 21. M. Genovese, Phys. Rev. A 71, 052314 **(2005)**.
 22. P. Traina, Open Systems & Information Dynamics 14(2), 217–222 **(2007)**.
 23. A. Vaziri, G. Weihs and A. Zeilinger, Phys. Rev. Lett. 89(24), 240401 **(2002)**.
 24. R. Thew, A. Acin, H. Zbinden, and N. Gisin, Quant. Inf. and Comp. 4, 93 **(2004)**.
 25. J.C. Howell, A. Lamas-Linares and D. Bouwmeester, Phys. Rev. Lett. 88, 030401 **(2002)**.
 26. T. Yang, Q. Zhang, J. Zhang, J. Yin, Z. Zhao, Z. Chen and J. Pan, Phys. Rev. Lett. 95, 240406 **(2005)**.
 27. D. Collins, N. Gisin, N. Linden, S. Massar and S. Popescu, Phys. Rev. Lett. 88(4), 040404 **(2002)**.
 28. J. L. Chen, C. Wu, L. C. Kwek, C. H. Oh and M. L. Ge, Phys. Rev. A 74, 032106 **(2006)**.

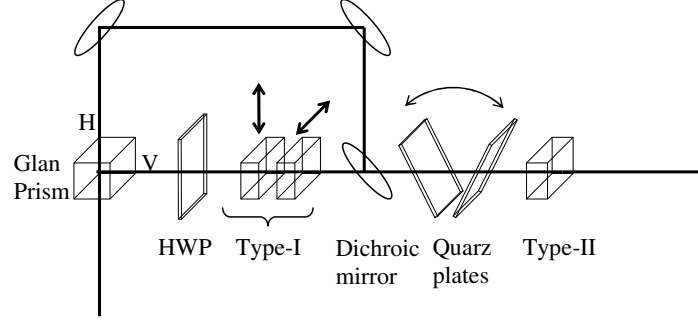


FIG. 2: Scheme for the production of polarization biphoton qutrits. A Glan-tompson prism splits the vertical and horizontal components of the UV pump beam. The first component, rotated by a Half-Wave Plate (HWP), pumps two type-I crystals whose optic axes are orthogonal to each other, while the horizontal component pumps a type-II

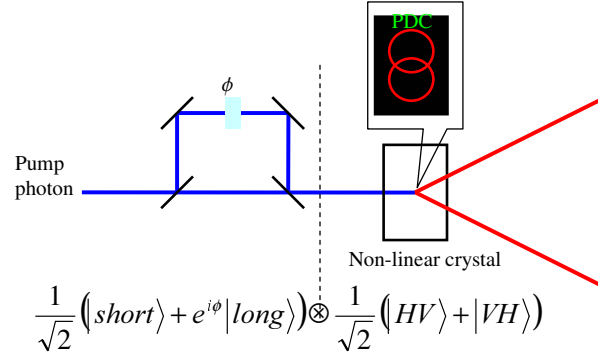


FIG. 3: Scheme of a proposed source of ququats by means of hyperentangled entangled photon pairs: PDC process splits a single photon, in a superposition state corresponding to the two possible optical paths of the Mach-Zender, in a pair featuring both polarization and time-bin entanglement.

29. A.V. Sergienko, Quantum Communications and Cryptography, Taylor & Francis, 2004.
30. N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, Rev. Mod. Phys. 74, 145–195 **(2002)**.
31. C. H. Bennett and G. Brassard, Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 175–179 **(1984)**.
32. A. K. Ekert, Phys. Rev. Lett. 67, 661–663 **(1991)**.
33. H. Bechmann-Pasquinucci and A. Peres, Phys. Rev. Lett. 85(15), 3313 **(2000)**
34. S. Pirandola et al., arXiv:0705.1099; C. Lupo, V. I. Man’ko, G. Marmo, J. Phys. A: Math. Theor. 40 13091-13100 **(2007)**.
35. D. Kaszlikowski, D. K. L. Oi, M. Christandl, K. Chang, A. Ekert, L.C. Kwek and C. H. Oh, Phys. Rev. A 67, 012310 **(2003)**.
36. H. Bechmann-Pasquinucci and W. Tittel, Phys. Rev. A 61, 062308 **(2000)**.
37. N. J. Cerf, M. Bourennane, A. Karlsson and N. Gisin, Phys. Rev. Lett. 88(12), 127902 **(2002)**.
38. N. J. Cerf, Phys. Rev. Lett. 84, 4497 **(2000)**.
39. P. W. Shor and J. Preskill, Phys. Rev. Lett. 85, 441 **(2000)**.
40. T. Durt, N. J. Cerf, N. Gisin and M. Żukowski, Phys. Rev. A 67, 012311 **(2003)**.
41. L. Mandel and E. Wolf, Quantum Coherence and Quantum Optics, Cambridge University Press, **(1995)**.
42. J. D. Franson, Phys. Rev. Lett. 62, 2205–2208 **(1989)**.
43. X. Ren, G. Guo, J. Li, C. Li and G. Guo, Chin. Phys. Lett. 23, 552 **(2006)**.
44. D. Stucki, H. Zbinden and N. Gisin, ArXiv: quant-ph/0502169v1 **(2005)**.
45. A. Mair, A. Vaziri, G. Wehls and A. Zeilinger, Nature (London) 412, 313 **(2001)**.
46. N. K. Langford, R. B. Dalton, M. D. Harvey, J. L. O’Brien, G. J. Pride, A. Gilchrist S. D. Bartlett and A. G. White, Phys. Rev. Lett. 93, 053601 **(2004)**.
47. X. F. Ren, G. P. Guo, Y. F. Huang, C. F. Li and G. C. Guo, Europhys. Lett. 76 (5), 753–759 **(2006)**
48. Y. I. Bogdanov, M. V. Checkova, S. P. Kulik, G. A. Maslennikov, A. A. Zhukov, C. H. Oh and M. K. Tey, Phys. Rev. Lett. 93 230503 **(2004)**.
49. M. D’Ariano, P. Mataloni and M. F. Sacchi, ArXiv: quant-ph/0503227v1 **(2005)**.
50. Y. I. Bogdanov, E. V. Moreva, G. A. Maslennikov, R. F. Galeev, S. S. Straupe and S. P. Kulik, ArXiv: quant-ph/0602138v1 **(2006)**.
51. L. Neves, G. Lima, J. G. Aguirre Gómez, C. H. Monken, C. Saavedra and S. Pádua, Physical Review Letters, 94 (10), 100501 **(2005)**.
52. X. F. Ren, G. P. Guo, J. Li and G. C. Guo, Phys. Lett. A 341, 81 **(2005)**
53. A. Cabello, Phys. Rev. Lett. 97 (2006) 140406; M. Barbieri et al., Phys. Rev. Lett. 97 (14), 140407 **(2006)**.
54. S. P. Walborn, S. Padua and C. Monken, Phys. Rev. A 68, 042313 **(2003)**.

55. M. Barbieri, G. Vallone, P. Mataloni and F. De Martini, Phys. Rev. A 75, 042317 **(2007)**.
56. G. Vallone et al., Las. Phys. 17, 993 **(2007)**.
57. J. Brendel, N. Gisin, W. Tittel and H. Zbinden, Phys. Rev. Lett. 82(12), 2594 **(1999)**.
58. M. Genovese and C. Novero, Eur. Phys. J. D 21, 109–113 **(2002)**.
59. C. Cinelli, M. Barbieri, R. Perris, P. Mataloni and F. De Martini, Phys. Rev. Lett. 95, 240405 **(2005)**.
60. G. Toth, J. J. Garcia-Ripoll Phys. Rev. A 75, 042311 **(2007)**; B. He et al., Phys. Rev. A 76, 042326 **(2007)**; M. Mirzaee et al., International Journal of Theoretical Physics 46, 1471-1494 **(2007)**.
61. A. Nb, Physics Letters A 362, 511, **(2007)**; H. J. Bernstein, Quantum Information Processing 5, 451 **(2006)**; G. Adesso and F. Illuminati, International Journal of Quantum Information 4, 383 **(2006)**; A. Miranowicz, Journal of Optics B - Quantum and Semiclassical Optics 7, 142 **(2005)**.
62. R.A. Bertlmann and P. Krammer, arXiv:0706.1743; H. Havlicek and M. Saniga, arXiv:0710.0941.
63. For the use of hyperentanglement in tests on the violation of local realism see also⁵³.
64. Here one can also mention recent studies on geometry of entanglement in qudits case, see⁶² and references therein.